**Testimony by**

**Paul Skare**

**Product Manager**

**Siemens Power Transmission & Distribution, Inc.**

**Energy Management & Automation**

**to the**

**U.S. Senate Committee on Homeland Security and Governmental Affairs**

**Subcommittee on Federal Financial Management, Government**

**Information, and International Security**

**July 19, 2005**

**Introduction**

Good afternoon Chairman Coburn, ranking member Carper, and members of the Subcommittee on Federal Financial Management, Government Information, and International Security. I am Paul Skare, Product Manager at Siemens Power, Transmission and Distribution, Inc. I am representing one of the manufacturers of SCADA (Supervisory Control and Data Acquisition) systems. My role at Siemens includes managing products for SCADA systems as well as substation automation systems. I am also involved in standards groups related to SCADA.

Siemens is one of the largest electronics companies in the world, operating in over 190 countries. We're a diversified company, delivering a wide array of products, systems and services in six main industries. These include information and communications, automation and control, power, healthcare, transportation and lighting. Siemens has over 70,000 employees in the United States across all 50 states.

Siemens' Energy Management & Automation provides software and technologies in regulated and deregulated energy markets. A key product for these markets is SCADA. SCADA collects information from devices in the power system, identifies problems, and allows users to remotely control these devices. Adding additional applications to a SCADA allows a more focused and enhanced solution for transmission or distribution systems (referred to as an Energy Management System (EMS) for transmission or a Distribution Management System (DMS) for

distribution).

My testimony today focuses on identifying potential security vulnerabilities of SCADA systems, the state of activities related to this, and recommendations to better protect those systems from harmful intrusion.

While our customers primarily use our SCADA systems for the electric system, some also use the same SCADA system for gas, water, and transportation systems. Although our systems are not used as commonly in other settings such as industrial control systems, the concepts are the same across all SCADA systems. In the appendixes of the written testimony, I have provided background information on SCADA and security issues relevant to SCADA. I would like to take this opportunity to congratulate the industry and the government in the work that has been done in the last three years in this area – it has started moving this work from the realm of art to science, and is finally starting to not only spread awareness, but also to get various players to talk the same language.

**SCADA Vulnerabilities**

SCADA vulnerabilities that may be a problem often involve issues associated with the following:

*Remote Access*

Remote access to SCADA systems is available for a variety of reasons: user access

outside of the control room, user support, and vendor support. This is a problem if there are any accidental (configuration of) security holes. If any backdoors are in the system (either leftover from the vendor or in place for user support), access points are easier to exploit. Local access points must be physically secure or these issues will also apply to them.

*Network configurations*

Network (and firewall) configurations are a very important aspect for SCADA systems. SCADA systems depend on a network for operational needs. If a firewall is bypassed accidentally or is miss-configured, a severe security hole could exist.

*Disgruntled employees*

If an employee becomes disgruntled, either before or after action by a utility (current or former employees), if the security process has not yet closed all access for that individual, the case for doing damage is greatest, since all the security in place can still be used by an authorized individual.

*Security holes, patches, viruses*

Systems rely on standard IT solutions [Commercial Off The Shelf (COTS)] to create a SCADA solution. Some third party security holes in operating systems, commercial databases and other applications can directly translate into security issues for the SCADA.

*Communication protocols not encrypted*

Communications, being the largest cost driver in a SCADA solution, is an important area. Since many field devices can last 30 or more years, utilities are reluctant to upgrade them unless there are clear needs. This means many old low power (computationally) devices are in operation, for which there are not standard, interoperable, commercial encryption solutions available. More modern communications methods, which introduce greater security risks, can move toward modern PKI solutions. Older methods still need a technical solution.

*Lack of incident reporting*

Since utilities are reluctant to share any data on security violations due to the negative publicity that is possible and the potential for this to do damage to stock prices, no clear picture of existing threats based on reliable metrics is available. The North American Electric Reliability Council (NERC) is working on creating a way to do this, but it is unlikely many incidents will be reported due to the negative publicity this brings to the utility. Similarly utilities are reluctant to share this information even with their SCADA vendors. This means that the SCADA vendors' view of the security threats may be understated. If reporting occurred, vendors would also be even more motivated to provide secure solutions due to negative feedback possibilities of their products.

**Challenges for SCADA installations**

- Single user sign-on procedures to track/audit user activity.

- Security toolkits to secure older products and verify the security with reports.
- Secure operating systems, databases, and applications.
- Interoperable PKI solutions needed for LAN/WAN communications.
  - Interfaces to other systems must be secured.
- Secure device protocols for LAN/WAN communications.
- Secure device protocols for synchronous/asynchronous communications.
  - Low computing power devices still need a technical industry solution that is accepted by NERC and utilities and interoperable between vendors.

**Recommendation: Business Process**

To be successful, a utility needs corporate security policies in place. Even the best security built in to a SCADA product is insufficient to prevent hacking of a SCADA system if not complemented with a strong security policy and security enforcement program by the users of the SCADA system themselves. This requires:

- A Security Manager
- A Security Awareness Program
- Periodic changes of Username / Password with specials content requirements
  - No More Yellow Sticky Notes!
  - Audits

Internal utility organization models also can impact security solutions. Often, SCADA systems are run within Operations, while the rest of IT is in a separate organization. This is due to the different needs of SCADA systems. SCADA Systems must process

information every two seconds and on demand, so a computer or communication problem cannot be tolerated for any great length of time. IT organizations are not typically suited to respond at the speeds required for SCADA systems. This means dedicated support people are used to support SCADA systems, but this introduces the possibility of disjoint security implementations between operations and IT. Business process within such organizations must be aligned for security solutions.

**Recommendation: Research**

Support the development of commercial encryption for old low powered devices that are now in operation. The energy industry still needs research for effective and economic encryption for low powered devices, (both wired and wireless), so RTU and other small devices can have encrypted communications. This must then be taken out to become industry standards endorsed by groups such as NERC.

**Recommendation: Reporting of both threats and incidents**

Promote more widespread reporting of security incidents. Keep this reporting confidential so that a Utility does not fear leaks to the media. Also, a secure way to share threat information with vendors and utilities is needed that does not impact national security. This increases awareness and helps justify investment from the private sector.

**Recommendation: Incentives for Utilities to secure their systems**

A tax incentive for securing critical infrastructure would be a positive approach to

encourage culture change at electric utilities.

**Recommendation: Federal and State cooperation**

Electric Utilities can not simply invest in all needed cyber security improvements due to the cost. It is not only a few computer systems that need to be addressed, but their entire control system infrastructure, from the Control Center on out to every monitored substation and on out to each field device (IED). Utilities need to be able to bring these costs into their rate structures, and this can not happen with out the support of each state's Public Utilities Commission. Also, non-jurisdictional utilities need to secure their systems as well.

**Recommendation: Continuing to merge the actions between DHS and DOE into a single cohesive action**

DHS and DOE have been cooperating, but as with any such large organizations there are still overlaps. This is evident at the National Labs. At Idaho National Laboratory, there is both the National SCADA Testbed (NSTB) (DOE), and the Control System Security and Test Center (CSSC) (DHS). These programs should be combined, and total funding increased for this valuable work. But also, the funding should be committed in advance for a five year period, so that the lab can also test the improvements made in the systems, until systems are judged to be secure. Competition between national labs such as INL, Sandia, PNNL and Oak Ridge for funding and programs should not create confusion in the eyes of the industry as it has in the past. Continued reorganizations and management changes combined with delays in

receiving funding have all contributed to overall delays in security enhancements over the last two years. Interestingly, the people I have met at DHS have been trying to go fast, efficient and cooperative in their work. To me this is a sign of a good culture at work in the organization.

**Recommendation: Embrace Risk based approaches to not only solving the problems, but also in allocating funds**

As a vendor, I represent my customers and their wishes, as well as my company's interests. As a taxpayer, I want to see the security issues resolved as efficiently and effectively as possible, and a risk based approach is the most effective and efficient.

**Conclusion**

Siemens strongly supports securing the nation's critical infrastructure in many ways. Siemens believes that as a responsible corporate citizen, we have advanced the state of the art in SCADA systems by openly discussing security issues with our customers through our customer association, by creating add-on products for older versions of our products (a Security Toolkit to harden existing installations – a leading innovation in our industry), by participating strongly in standards groups on security of SCADA system (IEC TC57 WG15; NIST PCSRF; DHS PCSF), by having a strong corporate focus on security, and by implementing security programs and standards in our products.

As a SCADA vendor, we have and will continue to develop, implement and advise on

enhanced features and technology to prevent security loopholes. However, in addition to built-in security features for SCADA, it is necessary to merge/complement it with an enterprise wide IT security policy and company cultures that support this. I believe that a form of compliance to security standards is required to truly safeguard the electric infrastructure of the United States. These standards will be most successful when created through open partnerships of government and industry.

In conclusion, I appreciate the opportunity to express the views of a leading SCADA manufacturer. We applaud your leadership in examining potential security vulnerabilities to America's vital infrastructure. We believe security compliance is a matter of corporate culture and that this culture must be set and influenced from the very top of every corporation to be effective. By starting at the top of management, I know that the culture of Siemens is one that supports security. We look forward to working with you and the subcommittee in building support for a broader understanding of critical information security issues.